CLAIMS

What is Claimed, is:

1. A method of operating a directory server system, comprising a directory server interacting with entries organized in a tree structure, in which said entries comprise user entries and role entries, ones of said role entries defining a role, and having an associated scope in the tree, the scope being defined from the location of said ones of said role entries in the tree, according to a predefined rule, with the role of an existing role entry being attached to a user entry subject to a first condition, which comprises a role membership condition and the fact that the user entry belongs to the scope of the existing role entry, the method comprising:

a) adding extra role data to the existing role entry, the extra data identifying an extra scope in the tree for the existing role entry,

b) attaching the role of the existing role entry to a user entry subject to a second condition comprising said role membership condition and the user entry belonging to the extra scope of the existing role entry.

2. The method of claim 1, wherein the existing role entry is an indirect role entry designating one or more other roles.

3. The method of claim 2, wherein the existing indirect role entry has an attribute designating the said one or more other roles.

4. The method of claim 1, wherein the role membership condition comprises the user entry having an attribute designating the role in the existing role entry.

5. The method of claim 1, wherein the existing role entry has a role filter condition, and the role membership condition comprises one or more attributes of the user entry meeting the role filter condition.

6. The method of claim 5, wherein the existing role entry has an attribute designating the role filter condition.

7. The method of claim 1, wherein said a) comprises:

a) adding the extra role data to the existing role entry in the form of an added attribute having a special attribute name and being associated with an attribute value identifying the extra scope.

8. The method of claim 7, wherein the value of the special attribute designates a location in the tree outside the scope as defined from said predefined rule, and further wherein the extra scope is defined from the designated location in accordance with a second predefined rule.

9. The method of claim 8, wherein the extra scope is defined as a subtree of the designated location.

10. The method of Claim 1, wherein the predefined rule comprises defining the scope of the existing role entry as a subtree of a parent of the existing role entry in the tree.

11. The method of Claim 1, further comprising:

c) responding to a request of whether a designated user entry has a given role by:

c1) determining a role entry corresponding to the given role,

c2) determining whether the designated user entry meets the first condition,

c3) if the designated user entry does not meet the first condition, determining whether the role entry has extra data identifying an extra scope, and,

c4) if the designated user entry does meet the first condition, determining whether the user entry meets the second condition.

12. The method of Claim 1, further comprising:

c) responding to a request for user entries having a given role by:

c1) determining a role entry corresponding to the given role,

c2) scanning the tree to determine user entries meeting the first condition,

c3) determining whether the role entry corresponding to the given role has extra data identifying an extra scope, and, if so, scanning the tree to determine user entries meeting the second condition.

13. The method of Claim 1, further comprising:

c) responding to a request for roles of a given user entry by:

c1) determining a role entry,

c2) determining whether the given user entry meets the first condition for the determined role entry,

c3) if the given user entry does not meet the first condition, determining whether the determined role entry has extra data identifying an extra scope, and, if so, determining whether the given user entry meets the second condition for the determined role entry, and

c4) repeating said c1) through said c3) with other roles entries until an end condition is met.

14. The method of claim 13, wherein the end condition comprises having scanned substantially all the applicable roles.

15. The method of claim 13, in which the given user entry belongs to a subtree of a top suffix of the tree structure, wherein:

said c2) is performed for each role belonging to the subtree of said top suffix, and

said c3) is performed for each top suffix of the tree structure, for each role belonging to the subtree of said top suffix.

16. A directory server system, comprising:

a directory server interacting with entries organized in a tree structure, said entries comprising user entries and role entries, ones of said role entries defining a role and having an associated scope in the tree structure, the scope being defined from the location of said ones of said roles entries in the tree structure, according to a predefined rule,

a role mechanism capable of attaching a role of an existing role entry to a user entry subject to a first condition, said first condition comprising a role membership condition and the user entry belonging to the scope of the existing role entry,

said role mechanism being further capable of determining whether said existing role entry has extra data designating an extra scope, and, if so, of attaching a role of the existing role entry to a user entry subject to a second condition, which comprises said role membership condition and the user entry belonging to the extra scope of the existing role entry.

17. The directory server system of claim 16, in which the existing role entry is an indirect role entry, designating one or more other roles.

18. The directory server system of claim 17, in which the existing indirect role entry has an attribute designating the said one or more other roles.

19. The directory server system of claim 16, wherein the role membership condition comprises the user entry having an attribute designating the role in the existing role entry.

20. The directory server system of claim 16, wherein the existing role entry has a role filter condition, and the role membership condition comprises one or more attributes of the user entry meeting the role filter condition.

21. The directory server system of claim 20, wherein the existing role entry has an attribute designating the role filter condition.

22. The directory server system of claim 16, wherein the extra data of the existing role entry comprise an added attribute having a special attribute name, and being associated with an attribute value identifying the extra scope.

23. The directory server system of claim 22, wherein the value of the special attribute name designates a location in the tree outside of the scope as defined from said predefined rule, and the extra scope is defined from the designated location in accordance with a second predefined rule.

24. The directory server system of claim 23, wherein the extra scope is defined as a subtree of the designated location.

25. The directory server system of Claim 16, wherein the predefined rule comprises defining the scope of a role entry as a subtree of a parent of that role entry in the tree.

26. The directory server system of Claim 16, wherein the role mechanism has a first function for responding to a request of whether a designated user entry has a given role, said first function being capable of:

i) determining a role entry corresponding to the given role,

ii) determining whether the designated user entry meets the first condition,

iii) if the designated user entry does not meet the first condition, determining whether the role entry has extra data identifying an extra scope, and,

iv) if the designated user entry does meet the first condition, determining whether the user entry meets the second condition.

27. The directory server system of claim 16, wherein the role mechanism has a second function for responding to a request for user entries having a given role, said second function being capable of:

i) determining a role entry corresponding to the given role,

ii) scanning the tree to determine user entries meeting the first condition,

iii) determining whether the role entry corresponding to the given role has extra data identifying an extra scope, and, if so, scanning the tree to determine user entries meeting the second condition.

28. The directory server system as claimed of claim 16, wherein the role mechanism has a third function for responding to a request for the roles of a given user entry, said third function being capable of:

i) determining a role entry,

ii) determining whether the given user entry meets the first condition for the determined role entry,

iii) if the given user entry does not meet the first condition, determining whether the determined role entry has extra data identifying an extra scope, and, if so, determining whether the given user entry meets the second condition for the determined role entry, and

iv) repeating said i) through said iii) with other roles entries until an end condition is met.

29. The directory server system of claim 28, wherein the end condition comprises having scanned substantially all the applicable roles.

30. The directory server system of claim 28 in which the given entry belongs to a subtree of a top suffix of the tree structure, wherein:

said ii) is performed for each role belonging to the subtree of said top suffix, and

said ii) is performed for each top suffix of the tree structure, for each role belonging to the subtree of said top suffix.

31. A computer readable medium having stored thereon instructions which when executed on a processor implement a method of operating a directory server system, comprising a directory server interacting with entries organized in a tree structure, in which said entries comprise user entries and role entries, each role entry defining a role, and having an associated scope in the tree, the scope being defined from the location of the role entry in the tree, according to a predefined rule, with the role of an existing role entry being attached to a user entry subject to a first condition, which comprises a role membership condition and the fact that the user entry belongs to the scope of the existing role entry, the method comprising:

a) adding extra role data to the existing role entry, the extra data identifying an extra scope in the tree for the existing role entry,

b) attaching the role of the existing role entry to a user entry subject to a second condition comprising said role membership condition and the user entry belonging to the extra scope of the existing role entry.

32. The computer readable medium of Claim 31, wherein the existing role entry is an indirect role entry designating one or more other roles.

33. The computer readable medium of Claim 32, wherein the existing indirect role entry has an attribute designating the said one or more other roles.

34. The computer readable medium of Claim 31, wherein the role membership condition comprises the user entry having an attribute designating the role in the existing role entry.

35. The computer readable medium of Claim 31, wherein the existing role entry has a role filter condition, and the role membership condition comprises one or more attributes of the user entry meeting the role filter condition.

36. The computer readable medium of Claim 35, wherein the existing role entry has an attribute designating the role filter condition.

37. The computer readable medium of Claim 31, wherein said a) of said method comprises:

a) adding the extra role data to the existing role entry in the form of an added attribute having a special attribute name and being associated with an attribute value identifying the extra scope.

38. The computer readable medium of Claim 37, wherein the value of the special attribute designates a location in the tree outside the scope as defined from said predefined rule, and further wherein the extra scope is defined from the designated location in accordance with a second predefined rule.

39. The computer readable medium of Claim 38, wherein the extra scope is defined as a subtree of the designated location.

40. The computer readable medium of Claim 31, wherein the predefined rule comprises defining the scope of the existing role entry as a subtree of a parent of the existing role entry in the tree.

41. The computer readable medium of Claim 31, wherein said method further comprises:

c) responding to a request of whether a designated user entry has a given role by:

c1) determining a role entry corresponding to the given role,

c2) determining whether the designated user entry meets the first condition,

c3) if the designated user entry does not meet the first condition, determining whether the role entry has extra data identifying an extra scope, and,

c4) if the designated user entry does meet the first condition, determining whether the user entry meets the second condition.

42. The computer readable medium of Claim 31, wherein said method further comprises:

c) responding to a request for user entries having a given role by:

c1) determining a role entry corresponding to the given role,

c2) scanning the tree to determine user entries meeting the first condition,

c3) determining whether the role entry corresponding to the given role has extra data identifying an extra scope, and, if so, scanning the tree to determine user entries meeting the second condition.

43. The computer readable medium of Claim 31, wherein said method further comprises:

c) responding to a request for roles of a given user entry by:

c1) determining a role entry,

c2) determining whether the given user entry meets the first condition for the determined role entry,

c3) if the given user entry does not meet the first condition, determining whether the determined role entry has extra data identifying an extra scope, and, if so, determining whether the given user entry meets the second condition for the determined role entry, and

c4) repeating said c1) through said c3) with other roles entries until an end condition is met.

44. The computer readable medium of Claim 43, wherein the end condition comprises having scanned substantially all the applicable roles.

45. The computer readable medium of Claim 43, in which the given user entry belongs to a subtree of a top suffix of the tree structure, wherein:

said c2) is performed for each role belonging to the subtree of said top suffix, and

said c3) is performed for each top suffix of the tree structure, for each role belonging to the subtree of said top suffix.